UNCLASS

DISA MLS Thin Client

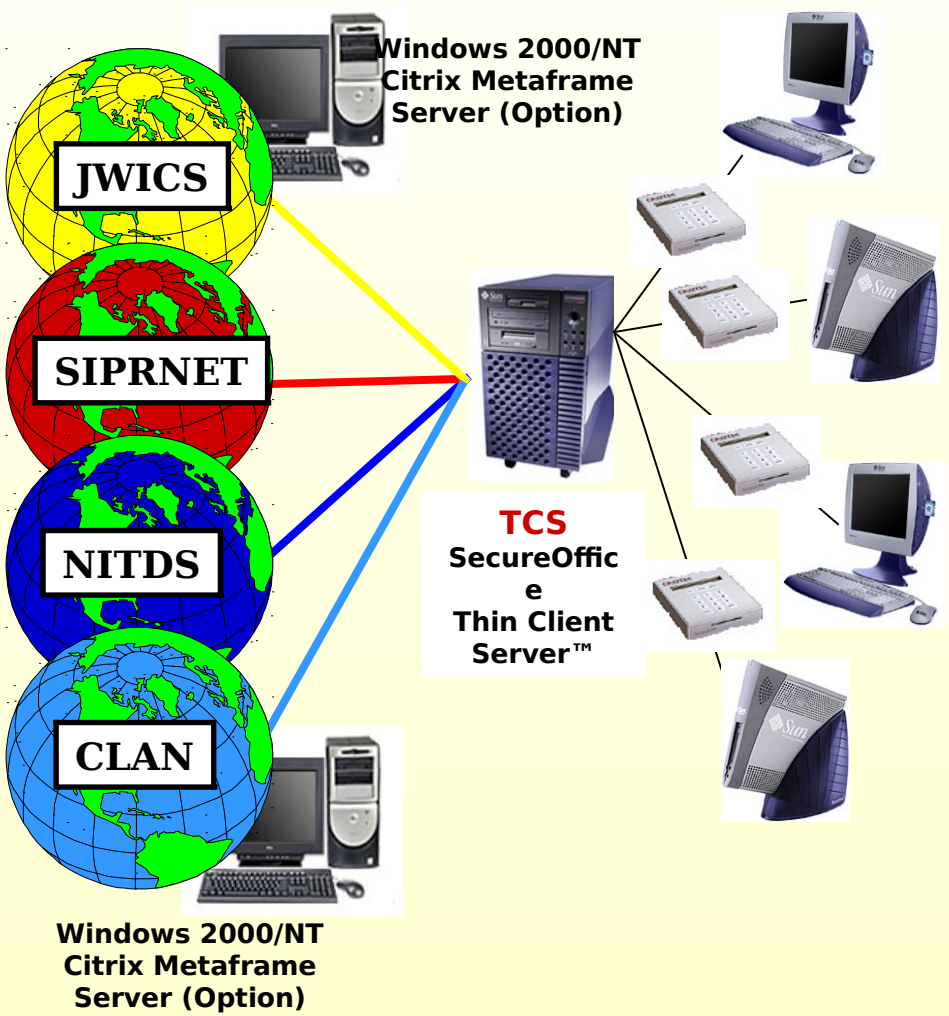
LCDR Edward G. Bryant
DISA/API4
February 2002

UNCLASS

Agenda

- Overview
- Functional
- Security
- Demonstration
- Summary

MLS Thin Client Architecture

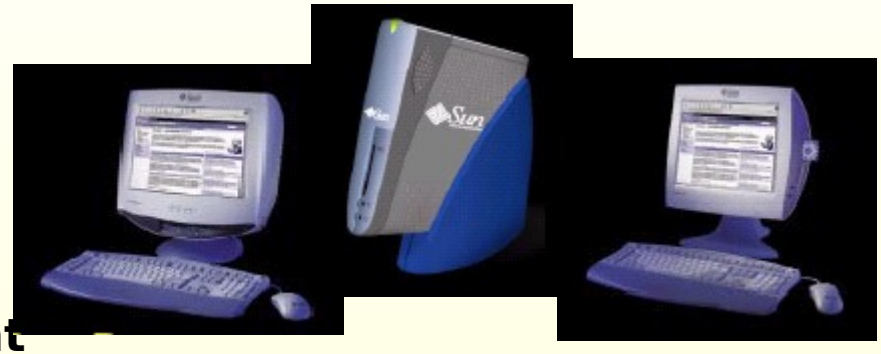


Features

- Sun SunRay Appliances (Ultra Thin Clients) execute applications simultaneously (at multiple classification levels) via SecureOffice Thin Client Server™:
  - Full Microsoft Windows 2000/NT application and network functionality via Citrix MetaFrame Server
  - E-mail, web browsing, and collaborative planning
  - Sun StarOffice
  - Sun SunForum
  - Trusted Relabeler™ Application
- Simultaneous access to resources and legacy servers on multiple classified networks
- Can integrate with Cryptek encryption devic
  - Provides encrypted path to distant clients

MLS Thin Client
Hardware

- **Appliance (Thin Clients)**
  - Built-in smart card reader
  - 4 USB ports
  - 100 MB Ethernet
  - Inexpensive-Very small footprint
  - Low Power-Energy star compliant



- **Session Server**
  - SecureOffice Thin Client Server
  - Trusted Solaris 8 &
    SunRay Session Server 1.3
  - Standard Sparc/Solaris server
  - 1-64 processors

Functional Overview

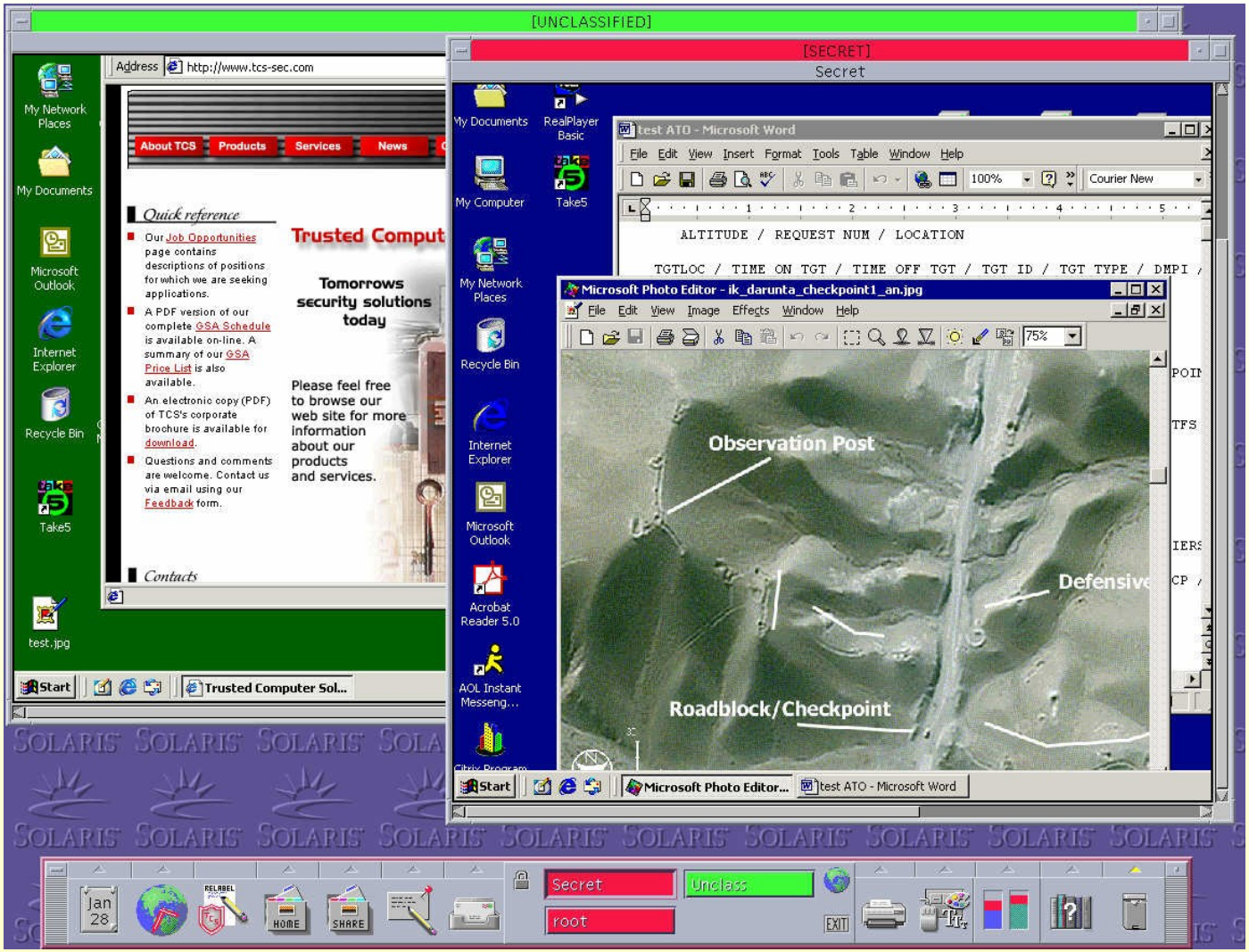
- Ops/Intelligence Workstation / Trusted Workstation / SecureOffice follow-on product (upgrade)
  - Based on previously accredited technology and proven CONOPS
  - Over 200 systems fielded and accredited
- Secure simultaneous connections to all LANs (at different security levels) from a single terminal via a single thin client terminal
  - Web Browsing, Email, etc.
  - Applications can execute simultaneously at all classification levels
- Provides ability to securely pass information between classification levels
- Full MS Windows functionality at multiple levels with the use of Citrix MetaFrame Servers -- obviates the need for multiple PCs on the desktop
- UNIX application support -- point-and-click, drag-and-drop interface

Functional Overview

- Based on Sun Microsystems SunRay Server/Client architecture
  - Reduced cost combined with reduced, administration, footprint, power, and maintenance/logistics tail
  - Centralized management (including MS Windows servers)
- Hot desk session mobility
- No client desktop maintenance or administration
- Increased desktop security
  - Diskless clients
  - Data encrypted to the desktop (with the use of Cryptek products)
- TCS provided GUI Administration Tools for Trusted Solaris management

SecureOffice™ Screenshot

UNCLASSIFIED
Labels are for example purposes only

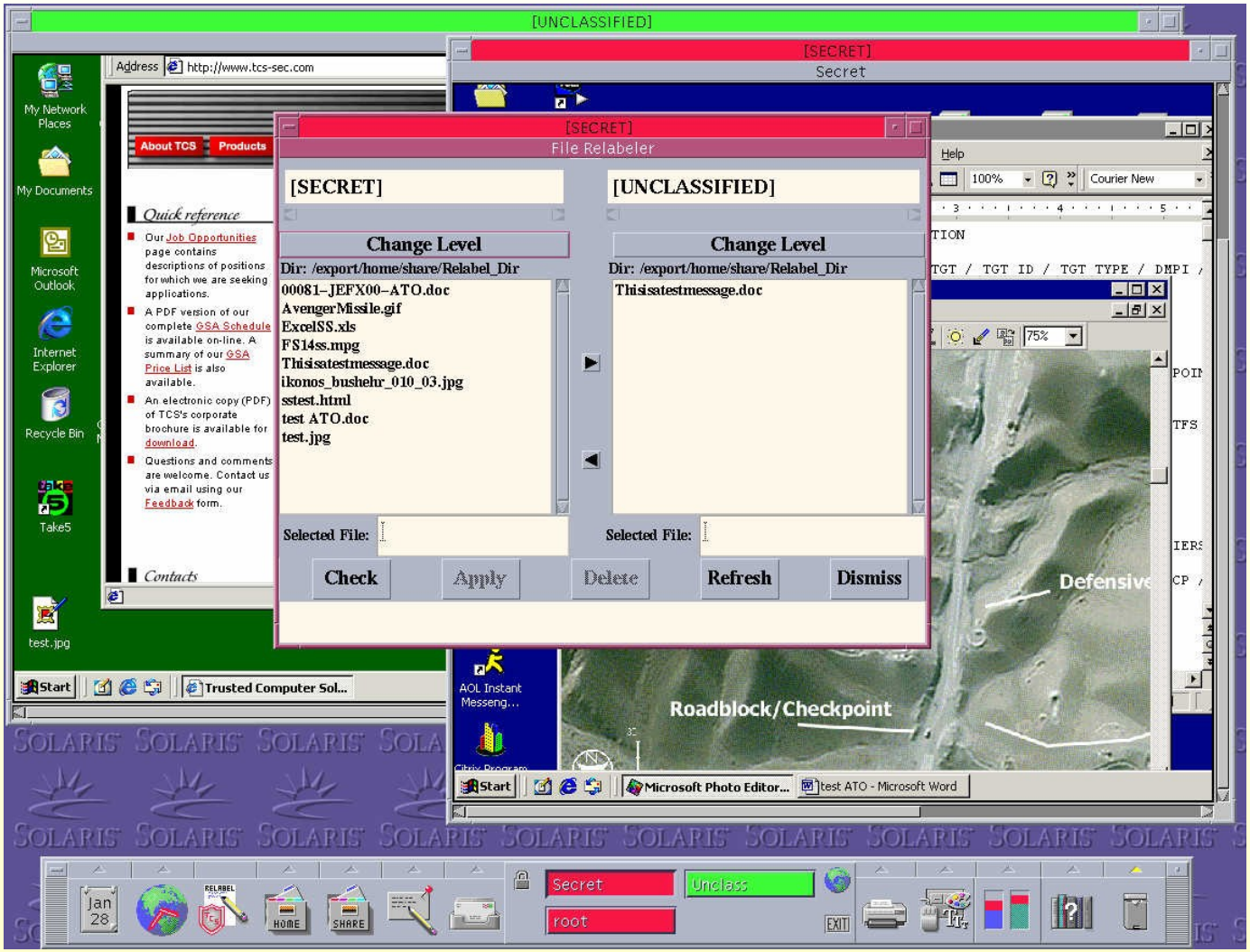

[UNCLASSIFIED]
[SECRET]
Secret
Address http://www.tcs-sec.com
About TCS
Products
Services
News
Quick reference
Our Job Opportunities page contains descriptions of positions for which we are seeking applications.
A PDF version of our complete GSA Schedule is available on-line. A summary of our GSA Price List is also available.
An electronic copy (PDF) of TCS's corporate brochure is available for download.
Questions and comments are welcome. Contact us via email using our Feedback form.
Trusted Comput
Tomorrows security solutions today
Please feel free to browse our web site for more information about our products and services.
Contacts
test ATO - Microsoft Word
ALTITUDE / REQUEST NUM / LOCATION
TGTLOC / TIME ON TGT / TIME OFF TGT / TGT ID / TGT TYPE / DMPI
Microsoft Photo Editor - ik_darunta_checkpoint1_an.jpg
Observation Post
Defensive
Roadblock/Checkpoint
Start
Trusted Computer Sol...
Microsoft Photo Editor...
test ATO - Microsoft Word
SOLARIS
Secret
Unclass
root
EXIT
HOME
SHARE

UNCLASSIFIED
Labels are for example purposes only

UNCLASS

SecureOffice™ Screenshot

UNCLASSIFIED Labels are for example purposes only



UNCLASSIFIED Labels are for example purposes only

UNCLASS

SECURITY OVERVIEW

- Upgrade based upon TCS' Ops/Intelligence Workstation / Trusted Workstation / SecureOffice line of products
  - DIA Accredited and NSA profiled baseline
  - Carried over verified software routines, secure configuration parameters, and software (where applicable)
  - Similar high level system architecture, connectivity, and CONOPS
- Executes on Sun Microsystems' Trusted Solaris 8
  - Common Criteria evaluated at EAL 4 level
  - Network and file/data labeling
  - Elimination of "superuser root" userid
  - User profiles incorporating privileges and authorizations
  - User profiles limit access to commands, desktop, and programs
- Specialized TCS GUI Admin tools eliminate insecure configuration caused by hand editing security tables
- Security-enhanced networking kernel that provides IP filtering capabilities

SECURITY OVERVIEW
(continued)

- IP filtering on all interfaces (built-in firewall)
  - Automatic configuration via TCS Network Interface Tool
- IP Forwarding disabled
- Restricted networking by configuration files, trusted networking tables, and firewall rules
- No remote user access allowed -- precludes penetration
- All Windows based application execute on a System-High Citrix MetaFrame servers

SECURITY OVERVIEW
(continued)

- Simple-to-use User Interface
  - Icon oriented actions
  - Drag-and-drop support
  - No UNIX commands necessary / No UNIX command line access
- Countermeasures engineered into system based upon previous vulnerability assessments by NSA and DIA
- Configuration management of all developed and integrated software
- A COTS product planned for use by a number of organizations
  - Assures compatibility and consistency between organizations
  - Full vendor support
  - A government and industry partnership

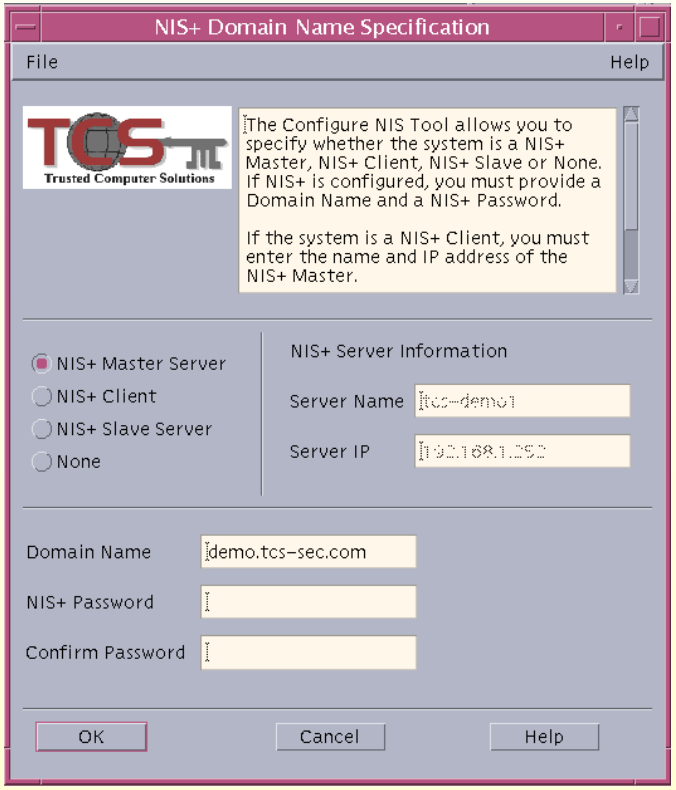
SecureOffice Thin Client™

System Administration

- GUI based Administration tools prevent inadvertent insecure settings by Administrator
- Centralized administration
- Simple TCS GUI tools for installation and configuring:
  - System Accred Range
  - NIS+ server/client
  - External Network Routes
  - Dirty Word Configuration
  - Network Interfaces
  - Remote Hosts / Nets
  - DNS Servers
- Use of Sun developed tools for other tasks, such as new user setup, printer and audit configuration

SecureOffice Thin Client™

Sample System Administration Tools


NIS+ Domain Name Specification
File
Help
Trusted Computer Solutions
The Configure NIS Tool allows you to specify whether the system is a NIS+ Master, NIS+ Client, NIS+ Slave or None. If NIS+ is configured, you must provide a Domain Name and a NIS+ Password.
If the system is a NIS+ Client, you must enter the name and IP address of the NIS+ Master.
NIS+ Master Server
NIS+ Client
NIS+ Slave Server
None
NIS+ Server Information
Server Name
tcs-demo1
Server IP
Domain Name
demo.tcs-sec.com
NIS+ Password
Confirm Password
OK
Cancel
Help

SECURITY OVERVIEW

(continued)

- Access to Administrative Configuration Tools are restricted to Administrative Roles
- Trusted GUI-based File Relabeler
  - Executes on Trusted Solaris
  - Dirty Word Search mandatory on all files (site configurable)
  - Dirty Word Search incorporated into non-text files (MS Word, PowerPoint, Excel, NITF image files (meta data search), GIF, JPEG, etc.)
  - StarOffice allows for previewing of files in MS Office format

SecureOffice Thin Client™

Protected Client LAN

- Can support VPNs to thin clients with Cryptek encryption devices
  - Provides data protection to clients outside secure spaces
    - Data protection for LANs traversing non-secure “gray” areas in the ship
  - Enabled with smart cards
    - Cryptek is working towards an integrated Cryptek/SunRay Client single reader solution
    - Beta version may be available for demonstration
  - Type II encryption

Summary

- Thousands of man-hours have been expended to make SecureOffice a secure, accreditable COTS solution
- Leveraged off of valuable lessons-learned from OIW-TWS development, certification, accreditation, and system fieldings
- Periodic security profiling techniques used during design and development to implement countermeasures
- COTS aspect of SecureOffice ensures commonality of fielded systems
  - Lessens time required by DAA to become proficient
  - Allows for Certification Testing of “deltas” vs. full formal Certification Test of entire system
  - Ensures full commercial support to sites by COTS vendor